IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

Mobile Botnet Detection A Machine Learning Approach using SVM

Pratik Dattatray Ambawale, Varun Vijay Wagh and Prof. Tejaswini Mali
Department of Artificial Intelligence & Data Science
ISBM College of Engineering, Nande, Pune, India
ambawalepratik@gmail.com,varunpatil0066@gmail.com
varunpatil0066@gmail.com , teju314@gmail.com

Abstract: *The security and privacy of smartphone users are seriously threatened by mobile botnets, which allow malevolent actors to carry out a variety of illegal actions, such as DDoS attacks, data theft, and resource exploitation. These mobile botnets are becoming more and more sophisticated, making it difficult to detect them with conventional signature-based and heuristic methods. This study proposes a machine learning-based method for mobile botnet detection that makes use of Support Vector Machines (SVM).The study focuses on behavioural feature extraction from mobile device system-level data and network traffic. The SVM model is used for classification once feature selection techniques have been used to select the most pertinent and discriminative attributes. The SVM model, making use of its capacity to manage nonlinear classification and high-dimensional data.Tests carried out on a variety of network traffic and system behaviour datasets gathered from mobile devices show encouraging outcomes for the detection of botnets. Compared to conventional detection techniques, the SVM classifier outperforms them in identifying mobile botnet activities with a high degree of accuracy, precision, and recall.The suggested SVM-based method improves mobile device security by offering a flexible and successful mobile botnet detection solution. The results of this study open the door to the development of strong and durable mobile security systems by providing insights into the proactive identification and mitigation of mobile botnet threats through the use of machine learning techniques.*

Keywords: Mobile Botnets, Machine Learning, Support Vector Machines (SVM), Botnet Detection, Smartphone Security, Behavioural Analysis, Network Traffic Analysis.

I. INTRODUCTION

The widespread use of mobile devices has completely changed how people interact, obtain information, and go about their daily lives. Smartphones are widely used, but this has also made them a desirable target for hackers looking to take advantage of security flaws and jeopardize user privacy. The rise of mobile botnets—networks of compromised devices used by hostile actors to carry out different illegal activities—is one of the most pernicious threats to mobile devices.Similar to their more established computer-based counterparts, mobile botnets pose a serious threat to cybersecurity. These covert networks use infected devices to perform a variety of malicious tasks, such as click fraud, spearheading denial-of-service (DDoS) attacks, and stealing confidential information.The ever-changing strategies used by mobile botnets are difficult to detect using traditional signature-based detection mechanisms and rule-based approaches, calling for more advanced and flexible techniques. The problem of mobile botnet detection may be effectively solved with machine learning's capacity to analyse massive datasets and spot complex patterns.

In order to provide a reliable method for mobile botnet detection, this research aims to investigate a machine learning technique that uses Support Vector Machines (SVM). The goal of the project is to train a support vector machine (SVM) model that can distinguish between actions linked to mobile botnets and those that are benign by using behavioural characteristics taken from network traffic and system-level data on mobile devices.The suggested SVM-based methodology has the potential to improve the detection capabilities in identifying mobile botnet activity because of its capacity to handle high-dimensional data and classify non-linear patterns. By offering a practical and efficient

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

method for identifying and reducing the harmful risks posed by mobile botnets, the research aims to further the field of mobile security.

This study clarifies the purpose and effectiveness of using machine learning for proactive mobile botnet detection by going over the methodology, experimental design, and findings from the SVM-based approach.

II. LITERATURE SURVEY

[1]Cooperative network behaviour analysis model for mobile Botnet detection: The growing threat of mobile HTTP botnets that target mobile devices with insufficient security is covered in the excerpt. It describes a model of cooperative network behaviour analysis that has been suggested to identify these complex mobile threats. By categorizing them according to the degree of periodicity and resemblance between group activities, this model seeks to detect the periodic communication patterns displayed by HTTP Botnets.To categorize the recurring behaviours of HTTP Botnets, three essential metrics were introduced. The initial metric is centred on the regularity with which mobile Bots communicate with their Botmaster; the other two metrics are based on group activity correlation and similarity analysis within a network.The suggested periodic classifier for HTTP botnets is effective in identifying their periodic behaviours; however, the paper notes that it has difficulties in differentiating these behaviours from those of regular applications that share similar patterns. A cooperative behaviour analysis technique was introduced as a remedy, looking at the correlation and similarity of group activities. The combined approach is more effective in identifying HTTP mobile Botnets, according to the results, with a low rate of false positives and a high accuracy and detection rate.

[2]Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks: In order to detect Android botnets, the paper presents an enhanced 1D Convolutional Neural Network (CNN). It can distinguish between regular apps and botnets thanks to training on static app features from a large dataset. Superior performance over existing machine learning classifiers was demonstrated during evaluation on a large number of real applications from the ISCX botnet dataset. High accuracy (98.9%), precision (0.983), recall (0.978), and F1-score (0.981) were attained by the CNN-based method, outperforming earlier research. It proves its superiority by successfully identifying novel, unseen Android botnets. In order to improve the CNN model's accuracy and efficiency in Android botnet detection, future work will focus on automating key parameter optimization.

[3]Detection of Mobile Botnets using Neural-Networks: This paper investigates the use of neural networks for the detection of sophisticated mobile botnets, also referred to as extremely dangerous malware. Challenges arise from the unpredictable behaviour of botnets, which are commanded by humans via peer-to-peer networks or C&C servers. Through an analysis of modern mobile botnets, common features were found and used to build a neural network training set. For efficient mobile botnet detection, the research presents a parallel architecture based on neural networks. This work, which is funded by several grants from the European Regional Development Fund and the Czech Ministry of Education, Youth, and Sports, advances cybersecurity research by identifying and mitigating mobile botnet threats.

[4]Astatic approach towards mobile botnet detection: The research focuses on developing defences against the growing threat posed by mobile botnets, especially on the susceptible Android operating system. An approach to static detection is put forth that makes use of machine learning algorithms to examine features from Android applications, including broadcast receivers, permissions, background services, and MD5. These characteristics support building a classifier to identify applications that may be able to operate as mobile botnets. Preliminary tests with the 14 malware families in the UNB ISCX Android botnet dataset show the effectiveness of this strategy. The study presents a thorough framework for categorizing applications as potentially benign or botnet-worthy using six different machine learning algorithms. In order to reliably detect applications that contain malware or malicious code, this ongoing study presents a four-layered comparison technique.

[5]Toward a Detection Framework for Android Botnet In order to detect Android botnets, the study suggests a technique that makes use of fresh features that can be distinguished from the security tiers of Android permissions. The study compared the performance of machine learning classifiers prior to and following the integration of the new feature set through experimentation. What sets this study apart from others is the tools it introduces to collect and analyze data from the Google Play Store, extract features, and pay attention to permission protection levels—a factor that has been neglected in other studies. The results showed that only the J48 classifier's performance was slightly enhanced by the new features, despite the Random Forest classifier performing better for both feature sets. Subsequent

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

research endeavors to perform a comprehensive examination to comprehend the importance of every feature in precisely identifying Android botnet applications, thereby augmenting forthcoming detection techniques.

[6]Detecting mobile botnets through machine learning and system calls analysis: The study emphasizes how mobile botnets pose an ever-growing threat and how detection is essential to reducing the risks associated with them. It aims to detect anomalous behaviours within mobile applications by presenting an anomaly and host-based approach that uses machine learning algorithms to analyse system call statistical features. The effectiveness of the method was demonstrated by testing on a self-generated dataset that included valid apps and different botnet families, with low false positives and high true detection rates. Strong performance across a range of metrics was achieved by the research using the Random Forest Classifier within a 500 ms time-window. It also revealed important characteristics of the classifier and the effects of various mobile botnet configurations on workflow. Looking ahead, the dataset will be enlarged, new botnets and legitimate apps will be added, and sophisticated machine learning methods will be used to improve classifier performance.

III. PROPOSED MODEL

The suggested model seeks to detect mobile botnets by utilizing machine learning techniques, particularly Support Vector Machines (SVM). The procedure entails taking system-level data from mobile devices and extracting features from network traffic. The following crucial steps are included in the model pipeline:

1. Gathering and preprocessing data:

Data collection from multiple sources, such as network traffic logs and system behaviors from mobile devices, is the first step in the process. The dataset used for training and testing is based on network packet captures and system-level logs that include application activities, communication protocols, and device-specific data.

2. Feature Extraction:

When separating legitimate activity from botnet-related activity, feature extraction is essential. Using feature extraction techniques, the gathered data is processed to extract pertinent attributes that represent the behavioral patterns displayed in mobile botnet activities. Possible discriminative factors include characteristics like system call sequences, communication patterns, traffic volume, packet size distributions, and communication patterns.

3. Feature Selection:

To improve the performance of the model and reduce dimensionality, feature selection algorithms are applied to the feature set that was acquired during the extraction phase. The most instructive and pertinent features are kept for mobile botnet detection using strategies like Information Gain, the Chi-squared test, or Recursive Feature Elimination (RFE)

4. SVM Model Training:

An SVM classifier is trained using the features that have been chosen. Using labeled data, the SVM modelwhich is well-known for its capacity to manage high-dimensional data and efficiently classify non-linear patternsis trained to produce a predictive model that can discriminate between activities related to botnets and benign ones..

5. Model Evaluation:

The suggested model is put through a rigorous evaluation process with respect to recognized metrics like F1-score, recall, accuracy, and precision. K-fold cross-validation is used to evaluate the model's performance in order to make sure it is robust against overfitting and generally applicable.

6. Experimentation and Analysis:

To assess the model's performance in detecting mobile botnets, it is put to the test on a variety of datasets. The model's ability to detect botnet-related activity while reducing false positives and negatives is evaluated using real-world network traffic and system behavior scenarios. The purpose of the suggested model in this study is to show how effective using SVM is for detecting mobile botnets. The study highlights how machine learning techniques can be used to improve mobile device security, covering the whole process from data collection to model evaluation.

IV. CONCLUSION

In order to address the urgent security concerns surrounding smartphone ecosystems, the study presented an in-depth exploration into the application of machine learning, specifically Support Vector Machines (SVM), for mobile botnet detection. By utilizing behavioral characteristics taken from system-level data and network traffic, the suggested SVM-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

based model showed encouraging results in detecting mobile botnet activity.The results of this study demonstrated the potential effectiveness of applying machine learning techniques to improve mobile device security. The SVM model demonstrated high accuracy and precision in distinguishing between activities related to botnets and benign activities after being trained on discriminating features obtained from various data sources. By reducing false positives and negatives, the SVM approach's resilience and flexibility made it a dependable method for proactive detection of mobile botnets.This research is important because it offers a promising methodology to counter the ever-evolving threats posed by mobile botnets. It also makes contributions to the field of mobile security. Through the utilization of machine learning models such as SVM, there is a chance to prevent malicious activities carried out by botnets against smartphone users, thus reducing the risk to user privacy and data security.There are some restrictions on the research, though. The dynamic nature of mobile botnet behaviors and the model's dependence on labeled data for training present difficulties for real-time adaptability and zero-day threat detection. Additionally, there may be practical difficulties in implementing the SVM model in real-world scenarios due to its scalability and computational requirements on mobile devices with limited resources.To improve the model's ability to adjust to changing mobile botnet behaviors, future research could focus on investigating ensemble techniques or deep learning architectures. Without depending only on labeled data, the model's capacity to recognize hitherto unseen botnet activities could be further enhanced by incorporating unsupervised learning techniques for anomaly detection.As a result of providing a reliable and proactive method of identifying mobile botnet activity, this research concludes that machine learning, and specifically SVM, has the potential to strengthen mobile security. In light of the constantly changing nature of cyber threats, the results provide a basis for further research and development into robust and flexible mobile device security solutions.

REFERENCES

[1]. M. Eslahi, M. Yousefi, M. V. Naseri, Y. M. Yussof, N. M. Tahir and H. Hashim, "Cooperative network behaviour analysis model for mobile Botnet detection," *2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, 2016, pp. 107-112, doi: 10.1109/ISCAIE.2016.7575046.

[2]. Suleiman Y. Yerima, Mohammed K. Alzaylaee"Mobile Botnet Detection: A Deep Learning Approach Using Convolutional Neural Networks". https://arxiv.org/abs/2007.00263, https://doi.org/10.48550/arXiv.2007.00263

[3]. Milan Oulehla, Zuzana KomínkováOplatková,DavidMalanik(2016). "Detection of Mobile Botnets using Neural-Networks". FTC 2016 - Future Technologies Conference 2016 6-7 December 2016 | San Francisco, United States

[4]. S. Anwar, J. M. Zain, Z. Inayat, R. U. Haq, A. Karim and A. N. Jabir, "A static approach towards mobile botnet detection," 2016 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, 2016, pp. 563-567, doi: 10.1109/ICED.2016.7804708.

[5]. Wadi' Hijawi, Ja'farAlqatawna, Hossam Faris. "Toward a Detection Framework for Android Botnet",2017 International Conference on New Trends in Computing Sciences, http://dx.doi.org/10.1109/ICTCS.2017.48

[6]. V. G. T. da Costa, S. Barbon, R. S. Miani, J. J. P. C. Rodrigues and B. B. Zarpelão, "Detecting mobile botnets through machine learning and system calls analysis," 2017 IEEE International Conference on Communications (ICC), Paris, France, 2017, pp. 1-6, doi: 10.1109/ICC.2017.7997390.